**Autores:**

CORBIERE, Emilio Federico y GÜIDA, María Clara

**Correo:**

fedecorbiere@gmail.com / mariaclaraguida@gmail.com

**Pertenencia institucional:**

Facultad de Ciencias Sociales - Universidad de Buenos Aires

**Eje temático:**

8 - Derechos de autor y copyright

**Título de la ponencia:**

©una de piratas: Cibercrimen, normativa y acciones antiterroristas en la era digital

**Palabras clave:**

Cibercrimen - Gobernanza - Terrorismo

---

## Introducción

El cometido de esta ponencia es avanzar sobre la caracterización y conceptualización de los llamados delitos informáticos o ciberdelincuencia/cibercrimen, la tipificación penal de los mismos y el surgimiento de regulaciones de carácter preventivo mediadas por el uso de redes digitales.

El problema central se focaliza en la falta de unicidad de criterios de tipo global y en donde el fin legitimo de la aplicación de las leyes entra en crisis con el llamado derecho universal -bajo resguardo en la Declaración Universal de los Derechos Humanos, 1948-. Sobre esta cuestión ya existen casos de intervenciones policiales directas, justificadas bajo el supuesto de prevenir delitos de "terrorismo" internacional.

De esta forma, se da especial observancia a cuestiones de alocación sobre la autoridad legal, efectos de territorio, nacionalidad, principios protectorios, personalidad pasiva, criterios de aplicación del derecho universal y su jurisdicción para "hacer cumplir" (*enforcement law*) el derecho internacional, tanto sea en forma de intervención directa o indirecta.

En este trabajo se releva la acción coordinada de fuerzas policiales -de tipo local y global- en donde se detecta un aprovechamiento de las tecnologías de vigilancia para perseguir delitos contra la propiedad intelectual, lo cual presume un uso solapado de

estos recursos a efectos regular la circulación de contenidos en las múltiples plataformas y soportes que posibilitan Internet.

La hipótesis de este trabajo plantea la existencia de un desplazamiento normativo que fuerza el "deber ser" de las llamadas leyes "antipiratería" hacia medidas "antiterroristas", en las que operan lógicas que avanzan sobre derechos humanos esenciales, y en los que resultan afectados la intimidad, la privacidad y los datos personales, bajo el fundamento de evitar eventuales delitos tecnológicos que se corresponden con la presunta intención de proteger la seguridad nacional/internacional.

## ¿Quién gobierna Internet?

Uno de los problemas asociados a la los delitos cibernéticos se focaliza en la historia de Internet y su crecimiento exponencial. Luego de que el financiamiento de los primeros sistemas de encriptación y paquetización de datos pasaran de la esfera militar al ámbito universitario y el comercial, la meca de las altas tecnologías se instaló en Silicon Valley (valles de silicio), California, en donde las empresas en formación (*start up*) se ubicaron a la par de las que serían las grandes corporaciones de Internet, como IBM, Intel y otras.

Desde entonces, ese parque industrial alberga no sólo a los principales jugadores del mercado cibernético, sino que opera como articulador de las políticas en comunicación que rigen el funcionamiento de las redes.

Situada también en California, ICANN (Corporación de Internet de Asignación de Nombres y Números) es la encargada desde 1998 de asignar los protocolos de Internet (TCP/IP) para la asignación de dominios (DNS), constituyéndose en un organismo transversal (Mastrini, De Charras y Fariña, 2008) que se rige bajo las leyes de ese Estado y de la Secretaría de Comercio de EEUU. Tiene su "libro verde" y un cuerpo colegiado de asesores con voz pero sin voto[1].

[1] No se trata de aquel manual de formación política que distribuyera el líder libio Muamar Gadafi para emular el "libro rojo" maoísta de la Revolución Cultural China ni el documento con idéntico nombre que presentó la Unión Europea para proteger el medio ambiente. En esta oportunidad, son las cláusulas elaboradas por el Consejo Nacional de Telecomunicaciones y Administración de Información (NTIA) del Dpto. de Comercio de EEUU, tendientes a mantener ciertas líneas de acción que hacen de Internet un ámbito privado, con políticas de participación e integración global.

En la práctica, empresas como Google -con una facturación anual en 2012 de u$s 38.000 millones de dólares y alrededor de 32.000 empleados[2]- ubican a figuras de su confianza en el Directorio. Vinton Cerf, uno de los fundadores de Internet y vicepresidente golbal de Google también preside el ICANN. Su contratación no resulta ingenua a los efectos de comprender la dimensión política de las legislaciones internacionales y frente a la insistencia de la UIT (Unión Internacional de Telecomunicaciones) por llevar la administración de la web a las Naciones Unidas[3].

En tiempos de juventud Cerf trabajó en los programas de investigación de la Universidad Stanford, financiado por la agencia gubernamental DARPA, dependiente del Departamento de Defensa de Estados Unidos. Por aquella época se discutía el diseño de multimodal de las redes digitales (ver cuadro: Topografía de las redes).

Estos elementos permiten dudar, al menos, de que Internet se constituya como una red libre, desde la cual los prestadores de servicio (ISP) garantizan un flujo de datos, sin restricciones con alojamiento bajo resguarda de privacidad, y la posibilidad de búsquedas e indexación y circulación abierta de contenidos.

Las sucesivas propuestas normativas sobre la propiedad intelectual impulsadas, desde el Parlamento norteamericano, entre 2011 y 2012, instalaron proyectos contrarios a la idea de libertad en Internet. Diversas iniciativas propician el filtrado de datos y bloqueo de sitios o aplicaciones (barreras de entrada en conexiones específicas) en nombre de la defensa de la propiedad intelectual o de la seguridad nacional. De todas estas medidas de restricción tecnológicas (*digital rights management*), se destaca el *traffic shapping* para restringir el envío de paquetes de datos por protocolos *End2End* (persona / persona) en redes descentralizadas.

¿Es legal que ocurra esto? ¿Quién califica la exigencia de la legalidad o el fin legítimo de estas acciones?

Supuestamente, el motivo principal de los acuerdos celebrados en Budapest busca penalizar la circulación de contenidos nocivos -como la pornografía infantil- e ilegales. No así, aquellos que incomoden a los gobiernos. Por tal razón, persiste en los supuestos de la regulación internacional una teoría del riesgo y la responsabilidad que

---

[2] Véase exposición de Henoch Aguiar en "Internet entre la libertad y el control global. El debate oculto del poder: la neutralidad en la red". Encuentro realizado en la Facultad de Ciencias Sociales (UBA), con la participación de Martín Becerra, Alejandro Piscitelli y Glenn Postolski, 08/05/2012. Disponible en http://youtu.be/stvYn_LSOJk, [Consulta: 31/06/2013].

[3] Véase síntesis del encuentro 2012, en http://www.itu.int/net/pressoffice/press_releases/2012/92-es.aspx#.UbTZnNjzbhM, [Consulta 31/06/2013]

obliga al paso de la mediación judicial, con lo cual el filtrado preventivo de información constituye una acción exepcional sobre la cual no existe magnitud de la necesidad si lo que se trata es de proteger las industrias culturales y la libertad expresión, cualquiera sea su plataforma comunicacional.

**Policías, piratas y conspiradores**

Tras la trama oculta de la "megaconspiración" investigada por el FBI -con intervención del Departamento de Justicia de Estados Unidos-, la detención de Kim "Dotcom" Schmitz por violación de derechos de autor y presunto lavado de dinero, se esconde la búsqueda o intento de creación de una policía global capaz de actuar de oficio en forma preventiva. El dueño de Megaupload resultó finalmente absuelto, en tanto los miles de clientes de ese repositorio digital nunca fueron resarcidos por los daños ocasionados por el secuestro de sus servidores raíz.

Este tipo de operaciones policiales transgreden la Digital Millennium Copyright Act (DMCA) estadounidense, la cual regula las infracciones sobre derechos de autor siguiendo las recomendaciones de la Organización de la Propiedad Intelectual (OMPI – ONU). No se trata de una normativa que recoja los principios de la cultura libre en Internet pero declara a sus proveedores como un "puerto seguro", y entiende que estos brindan un espacio neutral, por el que exime a los dueños de los canales de distribución (los proveedores ISP) de la responsabilidad por los negocios de sus clientes.

Entrada la segunda década del siglo, se conocieron varias iniciativas surgidas de sectores republicanos que encontraron consenso con el partido demócrata, tanto en la Cámara de Representantes como en el Senado norteamericano. Primero la Stop Online Privacy Act (SOPA), luego la Protect IP Act (PIPA) y, posteriormente, la Online Protection and Enforcement of Digital Trade Act (OPEN), entraron y salieron de las reuniones de *lobby* con empresarios del mundo informático y las industrias culturales.

SOPA obligaba a motores de búsqueda como Google a que borraran enlaces a páginas "sospechosas" y que colaboraran en la localización y persecución de quienes desconocían la autoridad en materia de derechos de autor. PIPA era una copia de la anterior, con la simple diferencia que en lugar de "obligar", "sugería". Estas formas de control, instaban además a empresas de publicidad como e-Bay o Pay Pal a poner barreras financieras sobre sitios "cuestionables". Esto ocurrió con el sitio WikiLeaks. La respuesta inmediata de la comunidad hackivista fue espejar cientos de sitios a las bases de datos filtradas por Julian Assange.

OPEN se trató de una solución “al paso” frente al rechazo de las empresas de Internet en constituirse como agentes de retención de información, lo que afectaba su modelo de negocios y por lo cual habían conformado la Net Coalition. En ella participaron Yahoo!, Google, Amazon, e-Bay, LinkedIn, Pay Pal, Twitter, Facebook, Skype, además de organizaciones como Humans Right Watch, Electronics Frontier Foundation, Mozilla, Reddit, WordPress y Wikimedia, entre otros. Su vocero fue Markham Erickson, un lobbista del mundo corporativo que suele ganar posiciones en el Capitolio.

Al no prosperar ninguna de las leyes, OPEN vino a intentar resolver la tensión y correr del grosero lugar que daba a los juzgados federales locales -dependientes del Departamento de Justicia- la potestad para actuar como si fuera una suerte de “Corte Global”, con la propuesta de crear una autoridad de aplicación en el ámbito de la Comisión de Comercio Internacional (ITC) de Estados Unidos.

En todos los casos se daba inmunidad legal sobre las responsabilidades ulteriores de abrir las bases de datos. La NetCoalicion se diluyó rápidamente y los jugadores de Silicon Valley se abrieron de los reclamos sobre los cuales avanzaban las organizaciones defensoras del acceso a la cultura y otros derechos humanos fundamentales.

Poco después se presentó la Cyber Intelligence Sharing and Protection Act (CISPA), que en castellano significa Ley de Protección e Información Policial Cibernética, esta repitió la primera receta de SOPA, dejando la posibilidad de que el gobierno de Barack Obama recopilara información de usuarios finales de Internet.

Ninguna de estas leyes pasaron las ruedas de discusión. Uno de los principales problemas para su sanción residió en el conflicto entre los modelos de negocio de Internet y la búsqueda de control político gubernamental. Las aplicaciones de Google se constituyen sobre bases de datos dinámicas para que su sistema AdWords reconozca términos relacionales con publicidades emergentes (*pop up* y otras). Según la firma sus servicios no violan el derecho a la privacidad ni las legislaciones locales al respecto. Por tal motivo, obligar a firmas como esta a constituir bases de datos estáticas afectaría la imagen de transparencia y respeto por los derechos civiles de su negocio.

Tras la ruptura de la NetCoalition surgió la iniciativa The Internet Defense League, donde las asociaciones WordPress, Reddit, Mozilla e Imgur organizaron apagones de Internet como forma de protesta patrocinadas por los especialistas de la Electronic Frontier Foundation y Public Knowledge.

Estas protestas no lograron mucho eco en el mundo ajeno a Internet. Las disputas continuaron y los gobiernos nacionales avanzaron sobre nuevas y estrategias hacia un universo orwelliano.

Al otro lado del Pentágono, la policía global Interpol propuso cuatro puntos a seguir: 1. Capacitación y formación (para la lucha contra la corrupción); 2. Incremento del apoyo operativo y de la ayuda a la investigación (neutralización de peligros incipientes e identificación de víctimas de catástrofes); 3. Innovación, investigación y seguridad digital (sobre ciberseguridad y ciberdelincuencia); y 4. Alianzas internacionales y desarrollo con los sectores público y privado. Esto tomó la forma de una encuesta que finalizó en noviembre de 2011, cuyos resultados serán analizados y entregados recién en la apertura del Complejo Mundial de Interpol para la Innovación en 2014, a realizarse en Singapur.

Mientras tanto el por entonces presidente de Egipto Honsi Mubarak ya había apagado por una semana el acceso a Internet, a comienzos de 2011, cerrando los sistemas con programas de inspección de datos. El FBI fue descubierto por la revista especializada C/net, con la revelación de la existencia de la Domestic Communications Assistance Center (DCAC), una unidad de inteligencia dedicada a pinchar teléfonos de autoridades locales, estatales y federales, incluyendo a proveedores de servicios de datos y redes sociales, cada vez que el Departamento de Justicia lo requiera. El informe muestra la existencia de solicitudes realizadas por dicha entidad de inteligencia para el financiamiento público de este programa en 2008[4].

## ¿Qué es la ciberdelincuencia?

Las primeras pistas del cibercrimen se dieron antes del atentado a las Torres Gemelas y casi al mismo tiempo de la masificación de computadoras para uso hogareño. Hacia 1996, mientras el entonces vicepresidente de Estados Unidos Al Gore recorría el mundo promocionando las "Autopistas de la Información" -como elemento clave para comprender los alcances de la nueva era digital-, el Comité para los Problemas de la Delincuencia (CDPC) del Consejo de Europa presentó el documento "Los problemas del derecho procesal penal en relación con la tecnología de la información". Allí se mencionaba la infracción a los derechos de autor como delito informático y la

---

[4] Véase “FBI quietly forms secretive Net-surveillance unit”, por Declan McCullagh, 22/05/2012. Disponible en http://news.cnet.com/8301-1009_3-57439734-83/fbi-quietly-forms-secretive-net-surveillance-unit/, [Consulta: 31/06/2013].

posibilidad de aplicar medias coercitivas sobre entornos tecnológicos, con allanamientos y secuestro de equipos.

Recién en 2001 se firmó Convenio sobre Cibercriminalidad de Budapest (aprobado por el Consejo de Europa el 23 de noviembre de 2001), único acuerdo internacional destinado a definir criterios normativos relevantes sobre delitos informáticos, que establece principios de equilibrio comunes en materia de derecho penal, procesal y en procura de promover Tratados de Asistencia Legal Mutua (MLAT) de cooperación internacional.

Un dato a tener en cuenta fue la sincronía con la normativa antiterrorista norteamericana, en particular la sección 215 de la Patriot Act (sancionada por una abrumadora mayoría en ambas cámaras del Capitolio, el 26 de octubre de 2001) la cual habilitó a organismos de inteligencia como la Agencia de Seguridad Nacional (NSA) a monitorear bases de datos, realizar búsquedas semánticas y revisar registros asentados en las empresas de comunicaciones, tanto de telefonía como en otros soportes.

El Convenio de Budapest entró en vigor el 1º de julio de 2004, habiéndose firmado previamente por el Comité de Ministros del Consejo de Europa (en su sesión nº 109, del 8 de noviembre de 2001). Cuenta con 45 firmas de los 47 países miembros del Consejo de Europa, a los que se suman 8 países observadores, entre los que figuran Estados Unidos, Japón, Canadá, Costa Rica, México y Sudáfrica.

La entrada de Argentina fue solicitada en marzo de 2010, durante la 5ta. Conferencia Anual sobre Ciberdelito (Estrasburgo). El 5 de octubre de 2011 por Resolución conjunta 863/2011 y 1500/2011 del Ministerio de Justicia y Derechos Humanos y la Jefatura de Gabinete de Ministros se creó la Comisión Técnica Asesora de Cibercrimen. No obstante ello, hasta la fecha de cierre de esta presentación nuestro país sólo estaba reconocido como miembro adherente[5].

Unos años antes los delitos informáticos fueron incorporados a nuestro Código Penal argentino mediante la Ley Nº 26.388/08. Allí se tipificaron aquellos actos realizados "con el fin de causar daño" que fueran mediados por procedimientos matemáticos. Su fundamento se encuentra en el mencionado instrumento internacional.

---

[5] Véase "Se creó una comisión asesora de cibercrimen", en Sala de Prensa, Jefatura de Gabinete de Ministros, Secretaría de Comunicación Pública del Gobierno de la Nación, 17/10/2011. Disponible en http://www.prensa.argentina.ar/2011/10/17/24787-se-creo-una-comision-asesora-de-cibercrimen.php, [Consulta: 31/06/2013].

Cabe destacar que el Convenio de Budapest se estructura en tres partes bien diferenciadas: una primera, en la que propone la tipificación como delito de algunas actividades *on line* -no previstas en los códigos procesales preexistentes-; una segunda, donde se afirma que los Estados deben exigir a las compañías operadoras de telecomunicaciones o servicios de transporte de datos -proveedores ISP- que realicen una vigilancia detallada del tráfico en las redes, incluyendo un análisis en tiempo real[6]; y, finalmente, una tercera en la que se exige la cooperación de los Estados en la investigación del cibercrimen mediante la posibilidad de compartir datos.

La segunda recomendación deja abierta la posibilidad de que se realicen bases de datos dinámicas y búsquedas semánticas de contenidos eventualmente peligrosos. También sirve a los efectos de justificar aquellas interpretaciones ambiguas donde los delitos informáticos, la piratería y el terrorismo entran en un mismo escenario que habilita el uso de la fuerza y el control social.

De esta forma, esta articulación normativa pretende resolver problemas político-institucionales de los gobiernos de turno, en lugar de promover regulaciones correctivas del pasaje de lo analógico a lo digital.

Según lo afirmado en el 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal (Salvador de Bahía - Brasil, 12-19 de abril de 2010), sobre "Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético", " (…) desde el decenio de 1960 hasta el de 1980, los Estados tuvieron que hacer frente a nuevos actos, tales como la manipulación informática y el espionaje de datos, para los que no había legislación penal. En esos años, el debate se centró en la elaboración de una respuesta jurídica. La introducción de la interfaz gráfica en los años noventa, a la que siguió un rápido aumento del número de usuarios de Internet, engendró nuevos desafíos. La información colocada legalmente en Internet en un país pasó a estar disponible en todo el mundo, incluso en aquellos países en que su publicación no era legal. Otro aspecto preocupante de los servicios en línea fue la rapidez del intercambio de información, que resultó ser especialmente problemática para la investigación de los delitos con dimensiones transnacionales. Si bien la información estadística es útil para poner de relieve la importancia constante o creciente de la cuestión, uno de los principales retos relacionados con el delito cibernético es la

---

[6] Véase Título V del Convenio referido a "Recogida en tiempo real de datos informáticos".

falta de información fidedigna sobre el alcance del problema y sobre las detenciones, los enjuiciamientos y las condenas correspondientes".

Para enero de 2011 se calculaba un número global de internautas cercano a los 2000 millones -sobre un estimativo de 7000 millones de habitantes-. Casi un tercio de la población mundial estaba conectada. Resta disociar el relieve sociológico de los cambios, en donde ciudadanos, gobiernos y empresas transitan por "sistema multiescalar de globalidades emergentes" (Sassen, 2007), en el cual las ciudades y sus bolsas de comercio constituyen circuitos, en permanente flujo, con tendencia a borrar las fronteras nacionales.

En esta tensión los mecanismos de actualización normativa sobre la propiedad privada (derechos de autor, patentes y marcas, entre otros) parecen cruzar al terreno de la llamada "seguridad nacional" en una suerte de retorno a la "guerra fría", en donde el terrorismo internacional es el principal pretexto para equiparar los delitos informáticos al ciberterrorismo.

## ¿Qué son los delitos informáticos?

Un delito informático es toda aquella acción típica, culpable y antijurídica ejecutada por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. De acuerdo con el Convenio de Budapest, los delitos pueden clasificarse en cuatro tipos diferentes: los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; los delitos relacionados con el contenido; los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines, y los delitos informáticos en general.

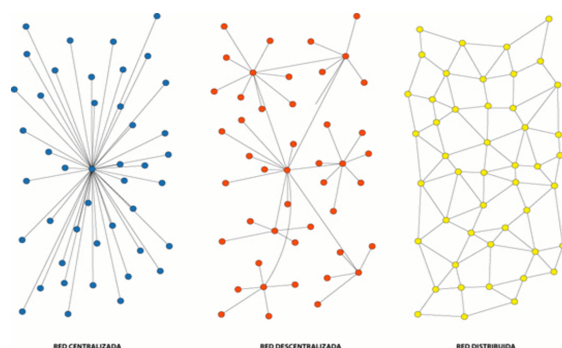
Desde 2008, en Argentina se puede perseguir con más precisión redes -virtuales- de pedofilia, conforme a los lineamientos de la Convención sobre los Derechos del Niño (ONU); la violación de bases de datos, contemplada tempranamente en la legislación argentina con la Ley 25.326, de Protección de Datos Personales; la difusión de pornografía infantil, la violación, intercepción o reenvío -no autorizado- de comunicaciones electrónicas -equiparadas al correo epistolar-; la suplantación de identidad y el fraude informático.

La regulación local sobre ciberdelincuencia nada dice respecto a la propiedad intelectual, habida cuenta que en 1998 el artículo 1º de la Ley 11.723/33 fue modificado por Ley 25.036, incluyendo los "programas de computación fuente y objeto". No

menciona el terrorismo internacional ni la implementación de medidas precautorias como la monitorización en bases de datos.

De esta forma, existe una diferencia entre el escenario local y el planteado por la Convención de Budapest, en el que subsiste la idea de un armado de redes de televigilancia.

Los delitos informáticos son, en gran medida, delitos de carácter transnacional, debido a la concepción reticular de Internet que hoy presenta una arquitectura distribuida.




Topología de las redes[7]

Las dificultades que el contexto transnacional plantea para la investigación de los delitos informáticos son, en cierto modo, similares a las que entrañan otros delitos globales.

En este sentido, las Naciones Unidas destacan que en el caso de la investigación de este tipo de delitos "*como consecuencia del principio fundamental de la soberanía nacional, según el cual no pueden realizarse investigaciones en territorios extranjeros sin el permiso de las autoridades locales, la cooperación estrecha entre los Estados involucrados es crucial*". A ello se agregan otras dificultades entre las que cabe destacar la referida al poco tiempo disponible para llevar a cabo las investigaciones de los mencionados delitos y la posible obstaculización de las investigaciones debido a procedimientos oficiales complejos y prolongados, motivo por el cual "el establecimiento de procedimientos para responder rápidamente a los incidentes y a las solicitudes de cooperación internacional se considera de importancia vital".

## ***Octopus CiberCrime* made in Argentina**

7

El 13 de junio de 2007 el Congreso Nacional aprobó la Ley Nº 26.268 (B.O. 5/7/2007), modificatoria del Código Penal en materia de asociaciones ilícitas terroristas y financiación del terrorismo, y de la Ley Nº 25.246 de Encubrimiento y Lavado de Activos de origen delictivo, sancionada el 13 de abril de 2000 (B.O. 10/5/2000). Dicha norma fue aprobada en el marco de las recomendaciones del Grupo de Acción Financiera en contra del lavado de dinero (GAFI), con el objetivo de evitar el lavado de dinero como fuente de financiamiento del terrorismo. La reforma estableció penas de prisión a quienes formaran parte de una asociación ilícita con fines terroristas -cuya tipificación ha sido sumamente controversial-.

Posteriormente, la ley fue modificada el 22 de diciembre de 2011, donde se derogó la figura de "asociación ilícita con fines terroristas", pero se agregó al Código Penal el artículo 41, que eleva al doble la pena en aquellos casos en que "*alguno de los delitos previstos en este Código hubiere sido cometido con la finalidad de aterrorizar a la población u obligar a las autoridades públicas nacionales o gobiernos extranjeros o agentes de una organización internacional a realizar un acto o abstenerse de hacerlo*".

Ante los cuestionamientos que suscitó este artículo, la Cámara de Diputados incorporó otro párrafo, con el cual se trató de reparar la denunciada ambigüedad del texto. En dicho agregado -que fue calificado de "superficial" por organismos de derechos humanos como el CELS- se estableció que los agravantes "*no se aplicarán cuando él o los derechos que se traten tuvieren lugar en ocasión del ejercicio de derechos humanos y/o sociales o de cualquier otro derecho constitucional*".

El artículo fue el punto neurálgico de una álgida discusión en el Senado puesto que, de acuerdo a varios legisladores opositores, "*la redacción del texto puede prestarse en el futuro para una interpretación criminalizante, ya que la deja librada al arbitrio de la autoridad de turno*". La Senadora por la Provincia de Salta Sonia Margarita Escudero (Peronismo Federal - FJV) y el Senador por la Provincia de Mendoza Ernesto Ricardo Sanz (UCR) realizaron las críticas más profundas a este artículo. Al momento de la votación, este último manifestó que "*se pretende disimular un problema de gestión con esta suerte de sobreactuación legislativa, que genera problemas de tipicidad penal y del principio de legalidad*". A su vez, el Senador por la Provincia de Santa Fe Rubén Giustiniani (Frente Amplio Progresista), consideró que "*es paradójico que la Argentina, un país a la cabeza en materia de derechos humanos, apruebe una ley que significa un grave retroceso*" y recordó que "*en Chile se utilizó recientemente la legislación antiterrorista promovida por el GAFI para criminalizar las protestas de la comunidad*

*mapuche (…) Esta ley significa un grave riesgo y habilita una persecución penal contra las personas y organizaciones que luchan por la reivindicación de derechos*".

Por su parte, los senadores oficialistas por las provincias de Entre Ríos y Neuquén Pedro Guastavino (PJ - FPV) y Marcelo Fuentes (FPV), respectivamente, remarcaron la necesidad de cumplir con las exigencias del GAFI y sostuvieron que "*hay suficientes garantías en nuestra estructura jurídica, en nuestro orden constitucional y en lo que conforma el cuadro de jurisprudencia para interpretar la norma en el alcance real que tiene*".

***Homeland***

Desde una década atrás diversas versiones periodísticas han confiado (sin revelar las fuentes) que el Departamento de Seguridad de EEUU (*Homeland Security*) tiene su lista de amenazas para prevenir el "terrorismo" internacional. El profesor universitario y experto en telecomunicaciones, Henoch Aguiar, ya había señalado en su libro *El futuro no espera. Políticas para la sociedad del conocimiento* (2007: 49-50) que las empresas del sector dejaban -a instancias del gobierno- "puertas traseras" o *back door* en los sistemas comunicacionales con el objeto de filtrar y jerarquizar términos "peligrosos" mediante buscadores semánticos.

El periódico digital Mail OnLine tuvo acceso a esa lista tras conocer un pedido de acceso a la información obtenido por el Centro de Información Privada Electrónica, un mecanismo que posibilita la FOIA (Acta para libertad de la Información, de sus siglas en inglés) que rige en EEUU desde 1967. En la difusa clasificación aparecen términos como "terrorismo", "ciudad Juárez" o nombres como "Felipe Calderon"[8].

En 2013 las agencias DPA, EFE y Reuters dieron a difusión -tras una publicación del diario británico The Guardian- otro escándalo por espionaje telefónico en EEUU sobre millones de líneas de la compañía Verizon. Según el diario la recolección masiva de datos en búsqueda de patrones de seguimiento, una orden firmada por el juez Roger Enson permitió que se espiaran 121 millones de usuarios

[8] Véase "Ciberespionaje: libertad vs. Control (Alt+33)", publicado en Agenda Digital, agencia Télam, 31/05/2013. Artículo fuera de línea. Disponible en el blog: http://bundest.wordpress.com/2012/05/31/ciberespionaje-assange-fbi/, [Consulta: 31/06/2013]

sobre los que se brindó la base diaria de lo que se llama “metadata telefónica”, luego del pedido “de una Corte de Supervisión de Inteligencia Extranjera secreta”[9].

La serie de televisión protagonizada por Claire Danes , la chica de *Terminator III: La rebelión de las máquinas*, muestra la docilidad de las mismas y que la realidad suele superar la ficción. En la primera temporada de *Homeland*, Danes, investiga mediante escuchas ilegales, a un marine converso por Al-Qaeda capturado durante la invasión de Afganistán y cautivo durante 10 años.

Además de los proyectos SOPA, PIPA, OPEN y CISPA, en Europa también hubo intentos por perseguir a usuarios de redes de Internet. Esta vez, a quienes se pronunciaron en las calles luego autoconvocarse por redes sociales. En abril de 2012 el presidente español Mariano Rajoy (del conservador Partido Popular) trató de contener los reclamos pacíficos del movimiento de “indignados” e instruyó a su ministro del Interior para reforme el Código Penal, con el objeto de calificar a las protestas convocas por Internet como “actos criminales”, identificando a los usuarios de plataformas de interacción virtual como una suerte de “guerrilla urbana” organizada.

Por entonces, el ministro en cuestión consideró como “terroristas callejeros” a los colectivos “antisistema” que protagonizaron noticieros y portadas de diarios durante los primeros meses de la crisis económica europea[10].

Gran Bretaña fue un poco más allá. El también conservador presidente David Cameron aceptó en abril de 2012, que el ministerio de Seguridad Interior (*Home Office*) estaba instrumentando la manera de vigilar “en tiempo real”[11] -como lo permite la Convención de Budapest- llamadas telefónicas, correos electrónicos en redes sociales, entre los que pueden destacarse Twitter y Facebook, pero también el chat de Blackberry y el popular software WhatsApp.

## Conclusiones

[9]Véase “Escándalo por espionaje telefónico a millones de personas en EE.UU”, sección internacionales, diario Ámbito financiero, 07/06/2013, p. 12.

[10] Véase Inglaterra: Gobierno planea una ley para monitorizar Inernet, RedEcoAlternativo. Disponible en http://www.redeco.com.ar/nv/index.php?option=com_content&task=view&id=7799, [Consulta: 31/05/2013]

[11] El número de internautas en el mundo supera 2.000 millones y el de abonados de la telefonía móvil 5.000 millones, sección Ciencia – Tecnología, agencia de noticias Ria Novosti, 26 /01/2011. Disponible en: http://sp.rian.ru/science_technology_space/20110126/148252875.html, [Consulta: 31/05/2013]

Hacia principios de la década del ’60, el ingeniero Paul Baran desarrolló las tecnologías de multiplexado para el envío y recepción de paquetes de datos. Sus trabajos asociados inicialmente a la inversión del complejo militar estadounidense en el proyecto Rand sirvieron al desarrollo de ARPANET, la red precedente a Internet. Lo interesante de su trabajo fue la conceptualización previamente señalada en tres tipos de redes: centralizadas, descentralizadas y distribuidas. Las primeras se corresponden a la lógica militar de aquellos tiempos: todo debía pasar por un nodo central. Las segundas, ya despliegan una matriz de tipo reticular, donde diversos puntos se transforman en espacios de interacción y ya no opera una lógica panóptica. Las últimas, por el contrario, al ser distribuidas subsisten a pesar de los intentos de control y la cancelación de nodos. En nuestro tiempo, la cultura de los consumidores finales de Internet transita por este tipo de plataformas, las cuales se multiplican exponencialmente según la cantidad de usuarios del sistema y rompen con las lógicas de control.

Los avances normativos que se han sucedido en los últimos años en materia de persecución sobre presuntos delitos de propiedad intelectual o la prevención de ataques terroristas pretenden retornar a ese universo centralizado que hoy produce problemas internos en las estructuras de gobierno, porque la cultura ha adquirido una topografía descentralizada.

Esa arquitectura no ha sido restringida a pesar del esfuerzo de organismos de inteligencia con las redes Echelon (dependiente de la NSA-EEUU), Emfopol (Unión Europea) y Carnivore (FBI-EEUU). Todas ellas han fracasado en su búsqueda de establecer criterios semánticos para identificar por términos sueltos que circulan por los sistemas de comunicación temibles redes de espionaje, que pongan en supuesto peligro la seguridad de las naciones. A falta de una “guerra fría” que justifique su existencia, los gobiernos vinculados al G-8 (Alemania, Canadá, Estados Unidos, Francia, Italia, Japón, Gran Bretaña, Rusia y otros de la Unión Europea), han buscado alternativas concretas y atajos legales como los problematizados en este trabajo.

Las leyes PIPA, ACTA, SOPA, OPEN, CISPA, han intentado trasladar a motores de búsqueda como Google y otras empresas privadas esa intencionalidad velada de controlar a los usuarios. Algunas de estas iniciativas, en especial el latente ACTA (Acuerdo Global Antifalsificación) y SOPA, promueven anular la mediación judicial para actuar de oficio sobre usuarios de Internet por eventuales delitos informáticos. ¿Constituyen éstos actos terroristas?

Como se mencionó al comienzo de esta ponencia, el sabotaje o *cracking* tipifica en Argentina, con la modificación del Código Penal por la Ley Nº 26.388/08, una posible violación “con el fin de causar daños”. Por fuera de la normativa hubo no pocos intentos de establecer sistemas de monitoreo urbano, instaurar mecanismos de geolocalización (que ya pueden realizarse a través de un *smartphone*), *domos* como el sistema SIBIOS que se discute instalar en nuestro país, entre otros. La localidad de Tigre ya implementó cámaras de vigilancia para su espacio público.

En los hechos, ya hubo experiencias de avance por tratados de asistencia mutua en los que nunca se aclaró a quién perseguía y los motivos. El principal autor internacional fue la agencia INTERPOL que, en un operativo conjunto realizó la Operación *Exposure* sobre España, Argentina, Chile y Colombia. Lo único que dejó esa megaoperación fue un simple ejercicio de amedrantamiento en el que, por ejemplo, de Argentina nadie quedó imputado de infracción alguna.

De esta forma, todo aquél que tenga una computadora con número de IP asignado tiene una chapa patente que lo identifica y puede ser desde Osama Bin Laden, el pajarito de Hugo Chávez y su Satán rojo rojito bolivariano, o un niño de 5 años jugando con el buscador de YouTube. Estos agentes del recontraespionaje son quienes ponen en peligro las democracias modernas.

El especialista en la materia Marcos Salt, integrante de la comisión asesora sobre Ciberdelincuencia, sostiene que el número IP no constituye identidad. No obstante ello, en los hechos las intervenciones policiales existen y, aparentemente, aquellas tecnologías de libertad que imaginaban una sociedad con instancias de democratización mediadas por su uso sufren del *enforcement law* que, en su acción directa, están tratando de imponer una restauración al control absoluto que se le escapó de las manos a quienes pensaron las redes digitales para la guerra ¿virtual?

La disputa va más allá de discusiones sobre "neutralidad en la red" o problemas de alocación de la autoridad legal. Está en el retorno a las redes centralizadas o su intento descrito ya descrito por Michel Foucault en su *Microfísica del Poder* (1980).

Lo cierto es que si se cae el nodo central también se apaga Internet, y con ello el ambiente de libertad relativa que por ahora invirtió aquel esquema que señalara el teórico venezolano Antonio Pascuali, cuando en los noventa aseguro que el “orden reina” para luego advertir con pasión, durante el Encuentro Panamericano de Comunicación -organizado por la Facultad de Ciencias Sociales de la UBA- que Internet es una “bomba de libertad”.

El desafío frente al avance continuo y la incorporación de las TIC en la cultura organizacional de los gobiernos y su adopción en las prácticas ciudadanas genera malos entendidos. En especial, aquellas regulaciones de tipo preventivo sobre un sujeto de legitimación pasiva difuso en donde no resulta claro observar cuándo se persiguen células terroristas, descarga de películas o redes de pedofilia.

Existen países que han procurado ejecutar políticas de control social desde la regulación de las industrias culturales, y otros que han mantenido reservas cuando las políticas en seguridad colisionan con otros derechos y garantías.

En este mundo incierto los brigadistas tecnológicos de Interpol y Europol se divierten practicando arrestos como los de la citada Operación Expusure. Los realizadores de *Homeland* están buscando argumentos para su tercera temporada tal vez inspirada en alguna versión autocontroda de un encierro en Gran Hermano. La cuenta de Twitter del bolivariano Nicolás Maduro fue supuestamente saboteada por cibercriminales peruanos presuntamente ligados a la célula hacker LulzSec; y, Kim Dotcom recibió las disculpas del gobierno de Nueva Zelanda -en septiembre de 2012- y anunció el lanzamiento de Megabox sin videos truchos de Locomía, para que Rajoy no pida su captura.

**Meta (Post) Data**

Al cierre de esta investigación, el académico y bloguero Enrique Dans sintetizó en "La magnitud del escándalo del Gran Hermano norteamericano"[12], la sumatoria de denuncias que pondrían al gobierno de B. Obama frente a un escándalo comparable con el caso Watergate, de escuchas ilegales durante 1972, por el cual Richard Nixon debió renunciar a su segundo mandato en 1974.

Durante los días previos diversos medios tradicionales y digitales condensaron hipervínculos a los precedentes de una saga de artículos publicados en el diario británico The Guardian, también sobre las pinchaduras de Verizon, ya mencionadas. En los medios hubo también referencias directas al caso de violación de la privacidad de periodistas de la agencia Associated Press y a la campaña para que Bradley Manning, no sufra la pena máxima de la corte marcial por haber entregado a WikiLeaks

[12] Véase en http://www.enriquedans.com/2013/06/la-magnitud-del-escandalo-del-gran-hermano-norteamericano.html, [Consulta: 10/06/2013]

documentos audiovisuales sobre crímenes de guerra ocurridos en las invasiones a Irak y Afganistán.

La última novedad, consiste en que esta vez Google y Facebook estarían involucradas en la entrega de sus registros, conforme a las solicitudes amparadas en el programa de inteligencia de la NSA, con supervisión de jueces y del Congreso estadounidense.

Todo, tras el paraguas legal de Prisma, un programa secreto de supervisión electrónica, vigente desde 2007 (clasificado con el número US-984XN), capaz de relevar lecturas de correo electrónico, video, chat de voz, imágenes, transferencia de archivos, notificaciones de inicio de sesión y contactos en redes sociales.

---

**Bibliografía**


Adorno, Theodor W. (1993) [1967]: "La educación después de Auschwitz", en revista Delito y Sociedad, N° 3, pp. 39-53. Disponible en: http://goo.gl/6lbFU [Consulta: 25-03-2013]

Aguiar, Henoch (2007): *El futuro no espera. Políticas para la Sociedad del Conocimiento*, Buenos Aires, La Crujía, pp 49-50. Disponible en: http://goo.gl/8BJWb

Aron, Raymond (1968) [1963]: *Paz y Guerra entre las Naciones*, Madrid, Alianza.

Braman, Sandra (2010): "The interpenetration of technical anl legal dicisio-making for the Internet", en *Information, Communication y Society*, pp. 309-329. Disponible en: https://pantherfile.uwm.edu/braman/www/bramanpdfs/57_interpenetration.pdf, [Consulta: 01-04-2013]

Braman, Sandra (2004): *The emergent global policy regime*, Palgrave Macmillan, (edición de autor).

Castells, Manuel (2001): *Internet, libertad y sociedad. Una perspectiva analítica*, Cataluña. Disponible en: http://www.uoc.edu/web/esp/launiversidad/inaugural01/intro_conc.html, [Consulta: 31-03-2013]

Cossio, Carlos (1944): L*a teoría egológica del derecho y el concepto jurídico de libertad*, Losada, Buenos Aires.

Hegel, Georg W. F. (1976): *Filosofía de la historia*, Buenos Aires, Claridad.

Hegel, Georg W. F. (1944) [1827]: *Enciclopedia de las Ciencias Filosóficas*, Buenos Aires, Ediciones Libertad.

Heller, Ágnes (1991): "De la hermenéutica en las ciencias sociales a la hermenéutica de las ciencias sociales", *Historia y futuro ¿sobrevivirá la modernidad?*, Barcelona, Península, pp. 19-57.

Kurbalija, Jovan y Gelbstein, Eduardo (2005*): Gobernanza de internet. Asuntos, actores y brechas*, Malta – Ginebra – Malasia, DiploFoundation. Versión PDF.

Lakatos, Imre (1983) [1978]: *La metodología de los programas de investigación científica*, Madrid, Alianza.

Lessig, Lawrence (2004): *Cultura libre. Cómo los grandes medios usan la tecnología y las leyes para encerrar la cultura y controlar la creatividad*. Disponible en: http://www.derechosdigitales.org/culturalibre

Mastrini, Guillermo; De Charras, Diego y Fariña, Cecilia (2011) [2008]. "Nuevas formas de regulación internacional y su impacto en el ámbito latinoamericano", en revista Electrónica Internacional de Economía Política de las Tecnologías de la Información y la Comunicación, Vol. 13, N° 3.

Merle, Marcel-Louise (1978). *Sociología de las relaciones internacionales*, Madrid, Alianza.

Morgenthau, Hans J. (1987) [1948]. *Política entre las naciones, la lucha por el poder y la paz*. Grupo Editor Latinoamericano.

Katz, Claudio (1999): "La tecnología como Fuerza Productiva Social: Implicancias de una Caracterización"; Quipú. Revista Latinoamericana de Historia de las Ciencias y la Tecnología, Vol. 12, N° 3, septiembre-diciembre, México.

Katz, Claudio (1998a): "El enredo de las redes. Un Análisis Crítico de M. Castells", Revista Voces y Culturas, N° 14, segundo semestre, Barcelona.

Kelsen, Hans (1965). *Principios del derecho internacional público*, Buenos Aires, El Ateneo.

Kelsen, Hans (1997) [1933]: *Teoría pura del derecho*, Buenos Aires, Eudeba.

Rogers, Everett M. [1962] (1974): *La comunicación de las innovaciones. Un enfoque transcultural*, Centro Regional de Ayuda Técnica, México-Buenos Aires.

Sassen, Saskia (2010). *Territorio, autoridad y derechos. De los ensamblajes medievales a los ensamblajes globales*, Buenos Aires, Katz.

Sassen, Saskia (2007). *Una sociología de la globalización*, Buenos Aires, Katz.

Shapiro, Carl y Varian, Hall R. (2000): "La Economía de la Información", en *El dominio de la información. Una guía estratégica para la economía de la Red*. Barcelona, Antoni Bosch Disponible en: http://www.antonibosch.com/system/downloads/505/original/ECSHAPIRO_Capitulo 1.pdf?1358337917, Consulta: 30-03-2013].

**Normativa:**

Declaración Universal de los Derechos Humanos. Disponible en: http://www.un.org/es/documents/udhr/

Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio (ADPIC - OMC) (1994). Disponible en: http://www.wto.org/spanish/docs_s/legal_s/27-trips_01_s.htm

Convención sobre la Protección y la Promoción de la Diversidad de las Expresiones culturales (UNESCO) (1995). Disponible en: http://unesdoc.unesco.org/images/0014/001429/142919s.pdf

Convenio sobre la Ciberdelincuencia (23/11/2001). Disponible en: http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.PDF

Ley 11.723 - Régimen legal de la Propiedad Intelectual. Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/40000-44999/42755/texact.htm

Ley de Delitos Informáticos, 26.388 (2008). Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

Ley de Proveedores de Servicios de Internet, 25.690 (2003). Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/80000-84999/81031/norma.htm

Ley de Servicio de Internet, 26.032 (2005). Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/105000-109999/107145/norma.htm

Ley 26.268, Modificación de la Ley Nº 25.246 de Encubrimiento y Lavado de Activos de origen delictivo. Asociaciones ilícitas terroristas y financiación del terrorismo. ("Ley Antiterrorista") Disponible en: http://infoleg.mecon.gov.ar/infolegInternet/anexos/125000-129999/129803/norma.htmPublicaciones periódicas:

"El FBI, Dotcom y su escape a la libertad", Disponible en: http://bundest.wordpress.com/2012/06/15/el-fbi-dotcom-y-su-escape-a-la-libertad/, 15/06/2012. (Publicado originalmente en la sección Agenda Digital de la agencia de noticias Télam, actualmente fuera de línea).

"Disputas globales por la administración de Internet", Disponible en: http://bundest.wordpress.com/2012/06/04/disputas-globales-por-la-administracion-de-internet/, 04/06/2012. (Publicado originalmente en la sección Agenda Digital de la agencia de noticias Télam, actualmente fuera de línea).

"Ciberespionaje, ¿made in Estados Unidos?", Disponible en: http://bundest.wordpress.com/2012/06/02/ciberespionaje-obam/, 02/06/2012. (Publicado originalmente en la sección Agenda Digital de la agencia de noticias Télam, actualmente fuera de línea).

"Ciberespionaje: Libertad vs. Control (Alt + 33)", Disponible en: http://bundest.wordpress.com/2012/05/31/ciberespionaje-assange-fbi/, 31/05/2012. (Publicado originalmente en la sección Agenda Digital de la agencia de noticias Télam, actualmente fuera de línea).

"Surge una Liga Global para defender los derechos digitales en la Web", Disponible en: http://bundest.wordpress.com/2012/05/28/surge-una-liga-global-para-defender-los-derechos-digitales-en-la-web/, 28/05/2012. (Publicado originalmente en la sección Agenda Digital de la agencia de noticias Télam, actualmente fuera de línea).

"¿El mundo avanza hacia una (ciber)policía global?", Disponible en: http://bundest.wordpress.com/2012/04/14/el-mundo-avanza-hacia-una-ciberpolicia-global/, 14/04/2012. (Publicado originalmente en la sección Agenda Digital de la agencia de noticias Télam, actualmente fuera de línea).

"Europa: Las convocatorias por redes sociales serán consideradas actos criminales", Disponible en: http://bundest.wordpress.com/2012/04/14/europa-las-convocatorias-por-redes-sociales-seran-consideradas-actos-criminales/, 14/04/2012. (Publicado originalmente en la sección Agenda Digital de la agencia de noticias Télam, actualmente fuera de línea).

"Guerra virtual", Disponible en: http://bundest.wordpress.com/2012/02/05/guerra-virtual/#more-864, 05/02/2012 (Publicado originalmente en la Revista Debate, actualmente fuera de línea).

"©Una de piratas", en diario digital Rebelion.org. Disponible en: http://www.rebelion.org/noticia.php?id=142421&titular=una-de-piratas-, 05/01/2012.